07/26/2010

RICOH

Technical Information:

@Remote Enterprise Pro Remote Communications Gate S Pro v1.0 White Paper

Document Version 2.0.0

Copyright © 2010 RICOH Americas Corporation. All rights reserved.

Notice:

THIS DOCUMENT MAY NOT BE REPRODUCED OR DISTRIBUTED IN WHOLE OR IN PART, FOR ANY PURPOSE OR IN ANY FASHION WITHOUT THE PRIOR WRITTEN CONSENT OF RICOH COMPANY LIMITED. RICOH COMPANY LIMITED RETAINS THE SOLE DISCRETION TO GRANT OR DENY CONSENT TO ANY PERSON OR PARTY.

Copyright © 2009 by Ricoh Company Ltd.

All product names, domain names or product illustrations, including desktop images, used in this document are trademarks, registered trademarks or the property of their respective companies. They are used throughout this book in an informational or editorial fashion only. Ricoh Company, Ltd. does not grant or intend to grant hereby any right to such trademarks or property to any third parties. The use of any trade name or web site is not intended to convey endorsement or any other affiliation with Ricoh products.

The content of this document, and the appearance, features and specifications of Ricoh products are subject to change from time to time without notice. While care has been taken to ensure the accuracy of this information, Ricoh makes no representation or warranties about the accuracy, completeness or adequacy of the information contained herein, and shall not be liable for any errors or omissions in these materials. The only warranties for Ricoh products and services are as set forth in the express warranty statements accompanying them. Nothing herein shall be construed as constituting an additional warranty. Ricoh does not provide legal, accounting or auditing advice, or represent or warrant that our products or services will ensure that you are in compliance with any law. Customer is responsible for making the final selection of solution and technical architectures, and for ensuring its own compliance with various laws such as the Gramm-Leach-Bliley Act, the Sarbanes-Oxley Act and the Health Insurance Portability and Accountability Act (HIPAA).

Version history:

Version	Issue Date	Revised item
1.0	Jan. 6, 2009	Initial release
2.0	July 17,2009	Added information about the communication between Remote Communication Gate S and devices for each function. The following changes were also made: 1. [Network usage] 1. Device Search: Added "The protocol/port is the same for all device types." 2. [Network usage] 1. Device Search: "NRS device" was changed to "@Remote Service device". 3. [Network usage] 1. RFU: Add "The Global Server does not access the Remote Communication Gate Pro server." 4. [Network usage] Other: Added information about max traffic amount. 5. [Data Flow/Data Storage] Other: Information about events generated by the Database was added. 6. [Data Flow/Data Storage] 1- Information about the encryption method used to store "Device data" was added. Information related to the Ricoh Private MIB was deemed unnecessary and was removed. 7. [Data Flow/Data Storage] Data flow chart removed was determined to be too complex, and was removed.

INDEX

1. What is Remote Communication Gate S Pro? 4
2. Glossary 4
3. Summary 5
4. System Overview 5
5. Network 6
5-1 Protocols and Ports used by the Primary Functions 6
5-1-1 Device Search 6
5-1-2 Local Device Search 7
5-1-3 Address Book and User Information Management 8
5-1-4 Update Printer Properties 9
5-1-5 Ping Test (Printer Properties) 10
5-1-6 Printer Properties' Reset Device 10
5-1-7 SNMP Trap Settings 11
5-1-8 SNMP Trap Reception 12
5-1-9 Device Polling (Status) 13
5-1-10 Device Polling (Tray/Toner Ink) 13
5-1-11 Device Polling (Other) 14
5-1-12 Device Polling (Counter) 15
5-1-13 Batch Configuration: 16
5-1-14 Remote Firmware Update 17
5-1-15 Device Log Transfer Settings 18
5-1-16 User Counter Collection 18
5-1-17 Device Job Log/Access Log Collection 19
5-1-18 Package Upload/Download 19
5-1-19 Other 20
5-1-20 Network Traffic Estimates 21
6. Attention 22
7. Data Flow and Data Storage 23
7-1 Data Storage 23
7-2 Other 25
8. JobLog / AccessLog Export Data 26

1. What is Remote Communication Gate S Pro?

Remote Communication Gate S Pro enables multiple devices in an organization to be easily managed, and for their operation costs to be reduced through improved efficiency.
Remote Communication Gate S Pro is designed to be used by IT administrators/operators and Ricoh CEs. As long as the Remote Communication Gate S Pro server can access the devices to be managed, the physical RCGSP server does not need to be located on-site.

2. Glossary

Word	Description
Ricoh CA	The server that issues certificates to @Remote service supporting devices and servers (Appliance).
Global Server	The Ricoh Server that provides firmware and other software.
RDH Authentication	Ricoh Original authentication service. This authentication is used for communication between the RCGSP Server and the Client PC, as well as between the RCGSP Server and any registered devices.
Package	An .exe file that can install multiple devices, drivers, and software.
Activation Server	The server that issues license keys.
RCGSP Server	Remote Communication Gate S Pro Server
Device	Indicates MFP and LP. (MFP= Multi Function Printer LP:Laser Printer)

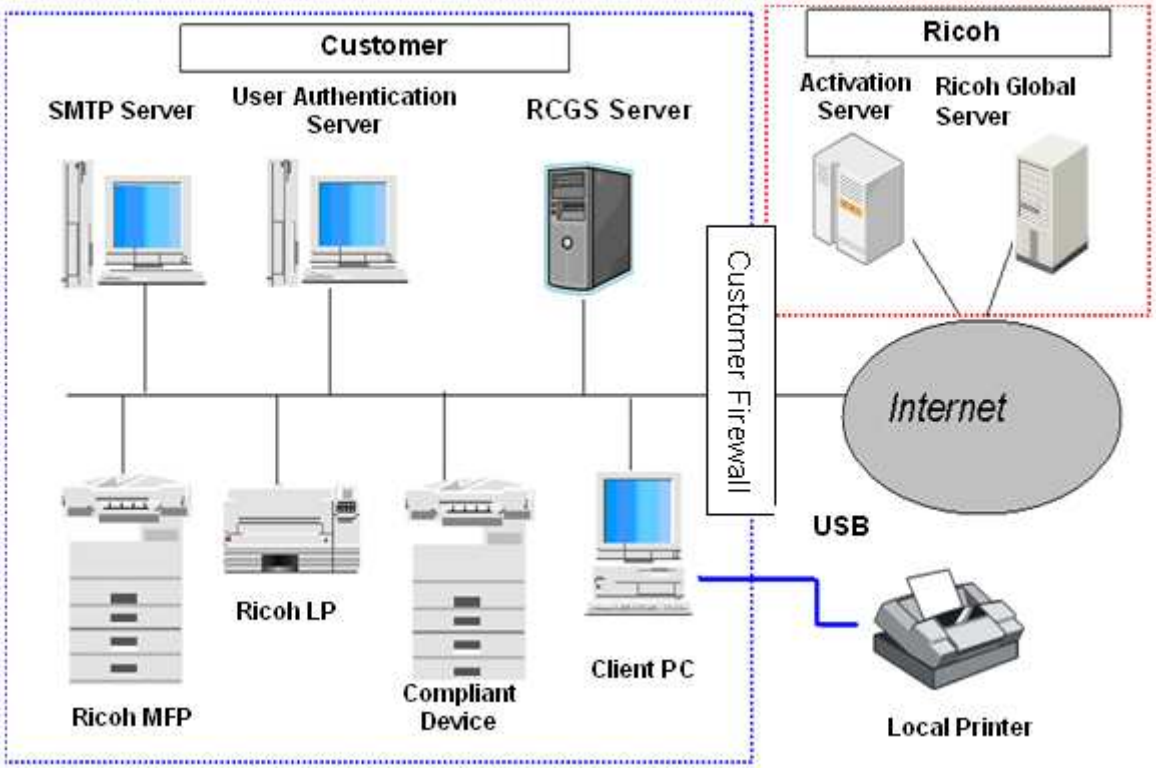
3. Summary

This Security White Paper describes the design of Remote Communication Gate S Pro in regards to network communication and information security. The information contained herein is intended for approved IT Management only.

This white paper does not include information on the @Remote Connector.
Please refer to the @Remote White Paper V7.0.0 for more information. Please contact a Ricoh sales representative to view the @Remote White Paper.

4. System Overview

The following image shows the network structure that Remote Communication Gate S Pro was designed for. This image shows the RCGSP server as inside the firewall, that is not required as long as RCGSP has access to any devices located inside the firewall.

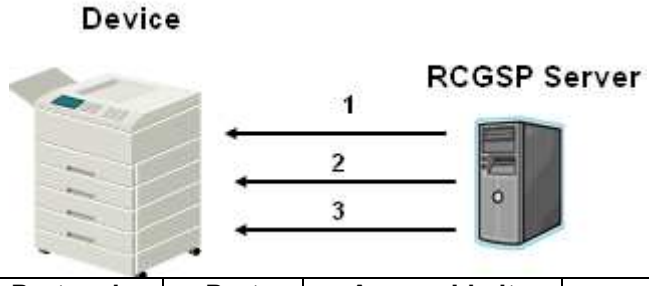


5. Network

5-1 Protocols and Ports used by the Primary Functions

5-1-1 Device Search

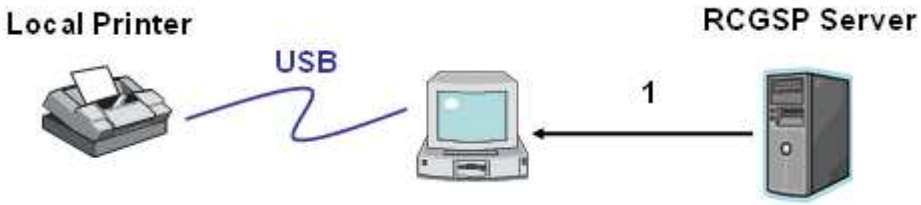
The RCGSP Server searches the specified network segment and attempts to discover any devices that exist in the specified segment. The image below describes the network communication flow when RCGSP communicates with a device during a Device Search.



No.	Process	Protocol	Port	Access Limit	Note
	Determine if device is communicating.	SNMP V1/V2	161	Requires : Read community name	**Collects the following information:** Device's Vender ID, Printer General Config Changes, Search Function. **Note:** Whether Ricoh device or not, SNMP uses the same port.
		SNMP V3		Requires : 1. User Name 2. Password 3. Authentication algorithm 4. Encryption password 5. Context name	
2	Check device for @Remote service support.	HTTPS/SOAP	7443	Requires: The certificate issued by the Ricoh CA (Certification Authority).	Device ID should be obtained when a @Remote supporting device is found.
3	Configure the Device Status Notification setting.				Non-Ricoh devices are not supported by this feature.

5-1-2 Local Device Search

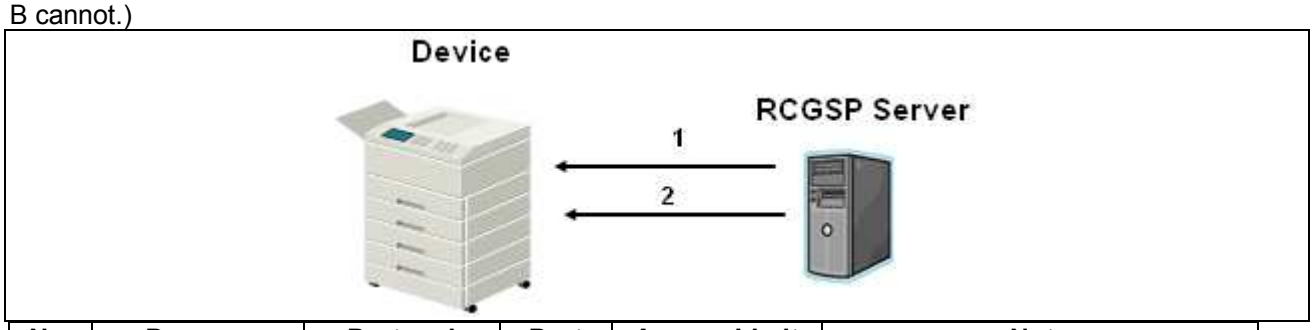
RCGSP Server searches client PCs in order to discover devices connected using USB.



No.	Process	Protocol	Port	Access Limit	Note
1	Determine if a USB device is installed on the target client PC.	SMB	TCP : 135, 139, 445 UDP : 137, 139	Requires: 1.User Name 2.Password If the PC is a part of Domain: 1. User Name (NetBios name or FQDN) 2. Password: Domain user's Password	**Collects the following information:** Serial Number Model Name Vendor Name Port Name Client PC's IP Address (Device has no IP address.)

5-1-3 Address Book and User Information Management

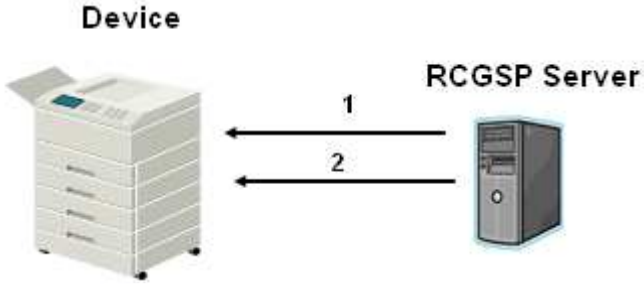
Address Book: User's mail address, Tel/Fax number and other information.
User Information: Used to restrict device functions per user. (Example: User A can use color printer but User B cannot.)



No.	Process	Protocol	Port	Access Limit	Note
1	Collect Information	HTTP/SOAP or HTTPS/SOAP	80/443	Requires: 1.User Name 2.Password	Collects the following information: 1. Capability ex. Max length of Login Name, Password policy, etc. 2. Address book and User Information.
2	Make settings changes.				Updates/Changes the following: 1. Address Book & User information

5-1-4 Update Printer Properties

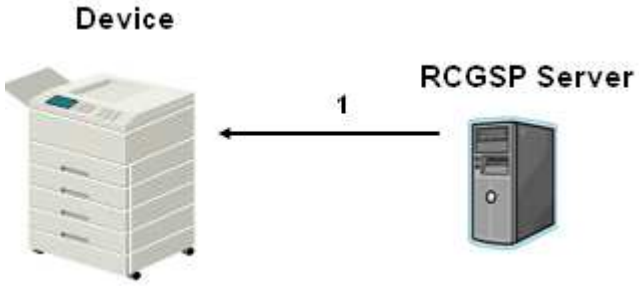
Updated Device data can be retrieved by the RCGSP Server during polling.



No.	Process	Protocol	Port	Access Limit	Note
1	Collects the following device information: -Device Status -Tray/Toner/Ink -Counter -Other	SNMP	161	Requires: -When SNMP V1/V2 is used: ->Community name -When SNMP V3 is used: 1.User Name 2.Password 3.Authentication Algorithm 4.Encryption password 5.Context name	-
2	Collects the device trap and log transfer information.	HTTP/SOAP or HTTPS/SOAP	80/443	Requires: 1.User Name 2.Password	-
3	Collect the device's counter information.	HTTPS/SOAP	7443	Requires: 1. The certificate issued by the Ricoh CA.	-

5-1-5 Ping Test (Printer Properties)

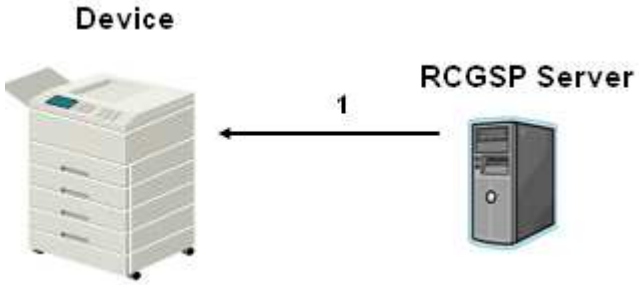
RCGSP Server can ping a device to check that the device and the server are successfully communicating.



No.	Process	Protocol	Port	Access Limit	Note
1	Send “Ping”	ICMP	-	-	-

5-1-6 Printer Properties’ Reset Device

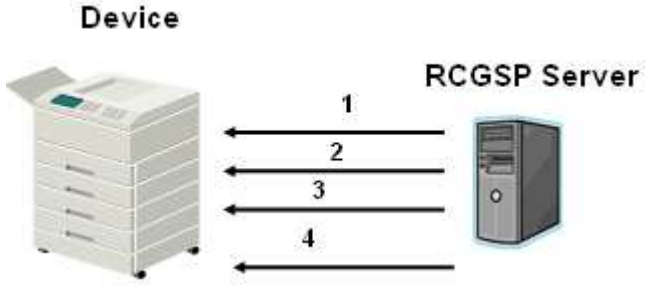
RCGSP remotely resets the device.



No.	Process	Protocol	Port	Access Limit	Note
1	Resets device information.	SNMP V1/V2	161	Requires: Write community name	-
		SNMP V3	161	Requires: 1.User Name 2.Password 3.Authentication algorithm 4.Encryption password 5.Context name	-

5-1-7 SNMP Trap Settings

When a device detects a problem (such as toner end), that device sends a SNMP trap (Network packet) to the RCGSP Server. The RCGSP Server then immediately polls the device in order to retrieve the error status. The following is a description of how RCGSP changes a device's Trap Settings.



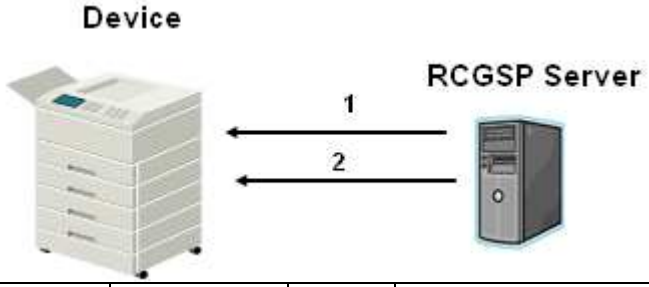
No.	Process	Protocol	Port	Access Limit	Note
1	Collect information.	HTTP/SOAP or HTTPS/SOAP	80/443	Requires: 1.User Name 2.Password	Collects the following information: 1.Capability ex. Max length of Login Name, Password policy, etc. 2.Current Settings
		SNMP V1/V2	161	Requires: 1.Read community name	Collects the following information (If necessary): 1.Current Settings
		SNMP V3	161	Requires: 1.User Name 2.Password 3.Authentication algorithm 4.Encryption password 5.Context name	
2	Send setting information.	HTTP/SOAP or HTTPS/SOAP	80/443	Requires: 1.User Name 2.Password	Sets the following information: 1.Setting value
		SNMP V1/V2	161	Requires: 1.Read community name	
		SNMP V3	161	Requires: 1.User Name 2.Password 3.Authentication algorithm 4.Encryption password 5.Context name	
3	Perform "Reset"	HTTP/SOAP or HTTPS/SOAP	80/443	Requires: 1.User Name 2.Password	Performs a "Reset" operation if necessary. Items 1-3 repeat as required.
4	Perform "Reset"	SNMP V1/V2	161	Requires: 1.Write community name	If necessary, perform one final "Reset".

		SNMP V3	161	Requires: 1.User Name 2.Password 3.Authentication algorithm 4.Encryption password 5.Context name	

NOTE: *SNMP Traps Support*
Older Ricoh devices only provide SNMP Traps for Printer MIB information. Newer Ricoh devices support SNMP Traps for both the Printer MIB and the Ricoh Private MIB. Please contact a Ricoh sales representative to determine which MIBs your devices support. Please note that the NIC used in the device must be a Ricoh approved card in order for SNMP Traps to function correctly.

5-1-8 SNMP Trap Reception

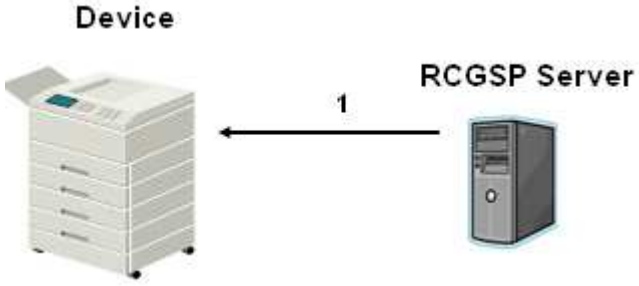
As described above, when a device encounters a status change it sends a SNMP Trap to RCGSP, and then RCGSP polls the device.



No.	Process	Protocol	Port	Access Limit	Note
1	Receive Trap	SNMP	162	Requires: -When V1/V2 is used: Community name -When V3 is used: 1.User Name 2.Password 3.Authentication Algorithm	The server waits 10 seconds before responding to a Trap.
2	Gather device status information via polling.	SNMP	161	Requires: When V1/V2 is used: Community Name When V3 is used: 1.User Name 2.Password 3.Authentication algorithm 4.Encryption password 5.Context name	A notification email may be sent depending on device's status and the notification settings.

5-1-9 Device Polling (Status)

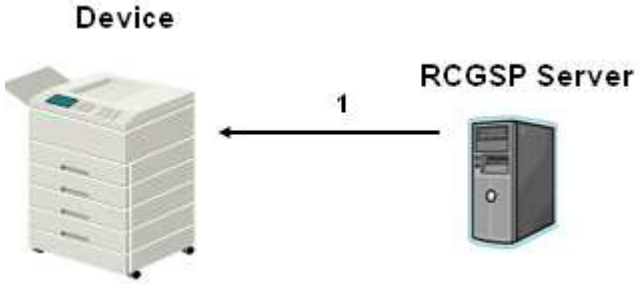
RCGSP polls the device for the most current status and stores it in the RCGSP DB.



No.	Process	Protocol	Port	Access Limit	Note
1	Gather device status information.	SNMP	161	Requires: When V1/V2 is used: Community Name When V3 is used: 1.User Name 2.Password 3.Authentication algorithm 4.Encryption password 5.Context name	A notification email may be sent depending on device's status and the notification settings. Frequency of the Email notification is depends on the polling interval and the device's status.

5-1-10 Device Polling (Tray/Toner Ink)

RCGSP Server polls the device for the current paper tray/toner/ink status and stores it in the RCGSP DB.



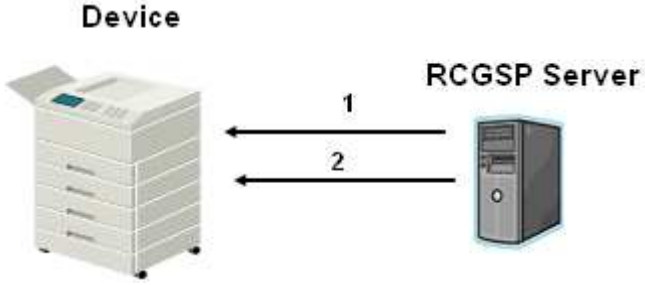
No.	Process	Protocol	Port	Access Limit	Note
1	Collect the device's Toner/Tray/Ink information.	SNMP	161	Requires: When V1/V2 is used: 1.Community Name When V3 is used: 2.User Name 3.Password 4.Authentication algorithm 5.Encryption password 6.Context name	-

Polling Limitations:

1. Only standard MIB information can be retrieved from 3rd devices by polling.
2. Please note that Polling and Discovery cannot run at the same time.

5-1-11 Device Polling (Other)

RCGSP polls the device for information stored on the device's HDD.



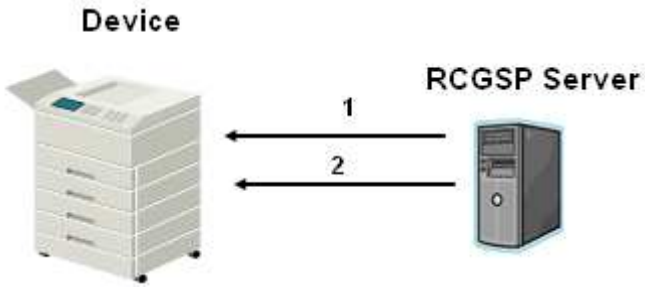
No.	Process	Protocol	Port	Access Limit	Note
1	Collect the device's printer version and trap setting information.	SNMP	161	Requires: When V1/V2 is used: Community Name When V3 is used: 1.User Name 2.Password 3.Authentication algorithm 4.Encryption password 5.Context name	-
2	Collect the device's trap setting and log transfer information.	HTTP/SOAP or HTTPS/SOAP	80/443	Requires: 1.User Name 2.Password	-

The following information is collected during Polling (Other):

Item
Log transfer information
IP Address
Physical Address
Document Box Free size
Web Image Monitor's note item
WIM Location item
System version
Host name
NIB version

5-1-12 Device Polling (Counter)

RCGSP Server polls the device for counter information.

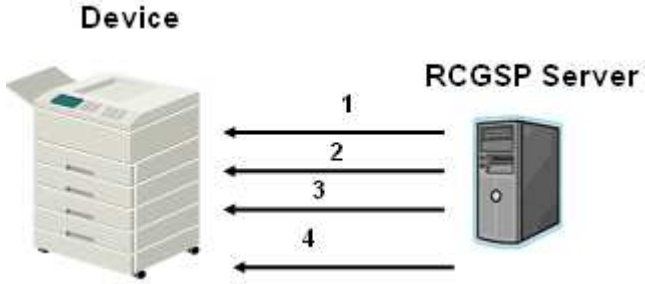


No.	Process	Protocol	Port	Access Limit	Note
1	Collects device counter information	SNMP	161	Requires: When V1/V2 is used: Community Name When V3 is used: 1.User Name 2.Password 3.Authentication algorithm 4.Encryption password 5.Context name	-
2		HTTPS/SOAP	7443	Requires: 1. The certificate issued by the Ricoh CA.	-

NOTE: *Recent Ricoh device: All counter types can be retrieved. Contact a Ricoh sales representative to determine if your device falls into this category.*
Non-Ricoh Device: Only total counter can be retreived.
Local Device: Counter information cannot be retrieved.

5-1-13 Batch Configuration:

Configures detailed device settings for multiple devices at once (network, device, email, protocol, authentication, etc.) and pushes those settings out to the selected devices. This function cannot be used with non-Ricoh devices.

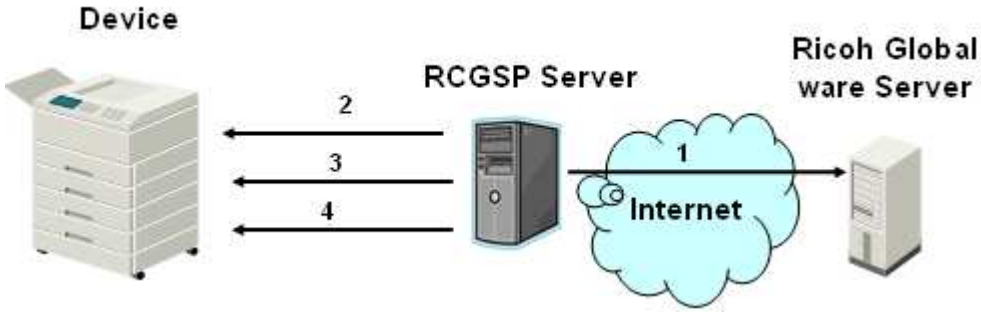


No.	Process	Protocol	Port	Access Limit	Note
1	Collect information.	HTTP/SOAP or HTTPS/SOAP	80/443	Requires: 1.User Name 2.Password	Collects the following information: 1.Capability ex. Max length of Login Name, Password policy, etc. 2.Current Setting
		SNMP V1/V2	161	Requires: 1.Read community name	Collects the following information (If necessary): 1.Current Settings
		SNMP V3	161	Requires: 1.User Name 2.Password 3.Authentication algorithm 4.Encryption password 5.Context name	
2	Send setting information	HTTP/SOAP or HTTPS/SOAP	80/443	Requires: 1.User Name 2.Password	Sets the following information: 1.Setting value
		SNMP V1/V2	161	Requires: 1.Read community name	
		SNMP V3	161	Requires: 1.User Name 2.Password 3.Authentication algorithm 4.Encryption password 5.Context name	
3	Perform “Reset”	HTTP/SOAP or HTTPS/SOAP	80/443	Need to set below: 1.User Name 2.Password	Performs a “Reset” operation if necessary. Items 1-3 repeat as required.
4	Perform “Reset”	SNMP V1/V2	161	Need to set below: 1.Write community name	If necessary, perform one final

		SNMP V3	161	Need to set below: 1.User Name 2.Password 3.Authentication algorithm 4.Encryption password 5.Context name	"Reset".

5-1-14 Remote Firmware Update

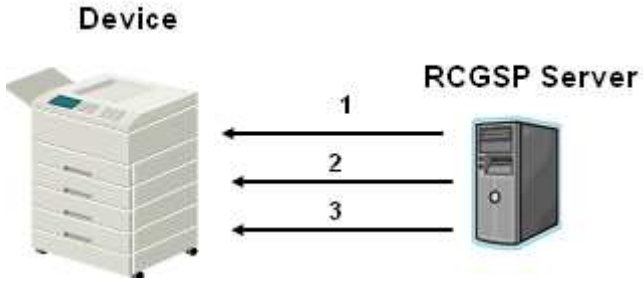
The RCGSP administrator can schedule the RCGSP server to contact the Ricoh Global Firmware server and download one of several versions of firmware. That firmware is stored on the RCGSP server, and then it is distributed to any devices targeted by the administrator.



No.	Process	Protocol	Port	Access Limit	Note
1	Download the Firmware	HTTPS	443	Original Authentication	・ Get the F/W ・ The RCGSP server is not accessed by Global Server.
2	Determine the port	FTP	(**A**) 10021, 10020 (**B**) 21, 20	**A** (Ports 10021 and 10020) requires the following: 1.User Name 2.Passowrd	**B** is used when **A** cannot be used. However, if **A** is used but encounters an access error, **B** will not be used.
3	Send the Firmware to device	FTP	Port No. that was used in No.2	-	-
4	Receive update results and updated version information.	FTP	Port No. that was used in No.2	-	-

5-1-15 Device Log Transfer Settings

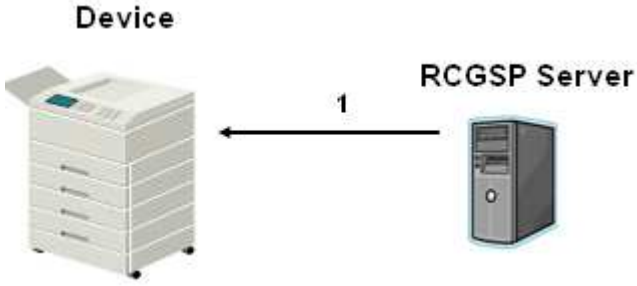
This function changes the settings used to determine if a device sends its Job Logs and Access Logs to the RCGSP DB for unified storage purposes. It also identifies the current status of log transfer settings per device.



No.	Process	Protocol	Port	Access Limit	Note
1	Collect information.	HTTP/SOAP or HTTPS/SOAP	80/443	Requires: 1.User Name 2.Password	Collects the following information: 1.Capability ex. Max length of Login Name, Password policy, etc. 2.Current Setting
2	Send setting information	HTTP/SOAP or HTTPS/SOAP	80/443	Need to set below: 1.User Name 2.Password	Sets the following information: 1.Setting value
3	Perform Reset	HTTP/SOAP or HTTPS/SOAP	80/443	Need to set below: 1.User Name 2.Password	Performs a “Reset” operation if necessary. Items 1-3 repeat as required.

5-1-16 User Counter Collection

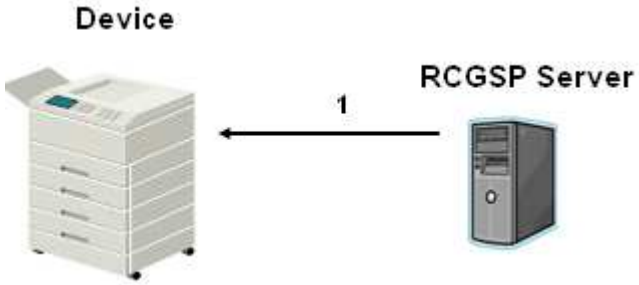
RCGSP server can collect user counter information from registered printers. User counters keep track of how printers are used on a per-user basis. Because these counters can require a large amount of disk space, collection is disabled by default. User counter information is not viewable from the Remote Communication Gate S web interface. The "UserCounterExport.exe" command line tool is used to export the data.



No.	Process	Protocol	Port	Access Limit	Note
1	Collect information	HTTP/SOAP or HTTPS/SOAP	80/443	Requires: 1.User Name 2.Password	Collects the following information: 1.Capability ex. Max length of Login Name, Password policy, etc. 2.User Counter

5-1-17 Device Job Log/Access Log Collection

Devices send their job logs and access logs to RCGSP Server immediately. However, RCGSP updates its DB every 60 minutes with the received log files.



No.	Process	Protocol	Port	Access Limit	Note
1	Receive device log	HTTP/SOAP or HTTPS/SOAP	Port No. chosen during installation.	Requires: ・RDH Authentication ・Certificate that was issued by the Ricoh CA. (Only for HTTPS)	1. Device sends the device log to Server. 2. The port cannot be changed after installation.

5-1-18 Package Upload/Download

Packager is a tool that creates a driver package for simplified driver installation and setup (RPCS, PCL LanFax, RPCS Raster) and utility(DeskTopBinder, Smart Device Monitor) for the end user.

No.	Process	Protocol	Port	Access Limit	Note
1	Download the Packager application from the server.	HTTP/HTTPS	Port No. chosen during installation.	RDH Authentication	Browser -> Apache or IIS
2	Upload a package to the server using the Packager application.	HTTP/HTTPS		RDH Authentication	Packager -> Apache or IIS
3	Distribute the uploaded package by email.	SMTP V1	25	SMTP Authentication	Port 25 must be open.
		POP	110	Pop Authentication	If using POP Authentication is selected, port 110 must be open.

5-1-19 Other

Describes the various types of network connections between the RCGSP server and the other network entities with which it interacts.

〔Client PC ->Remote Communication Gate S Pro Server〕

No.	Process	Protocol	Port
HTTP/HTTPS	Port No. chosen during installation.	RDH Authentication	Browser → Apache or IIS
HTTP/HTTPS			Packager → Apache or IIS
DCOM	4000~4010		Authentication Manager → Remote Communication Gate S Server (ServerAgentService)

〔Remote Communication Gate S Pro Server-> External Authentication Server (LDAP)〕:This authentication is used when logging in to RCGSP's web browser interface.

Protocol	Port	Access Restriction	Note
LDAP LDAPS	389 636	LDAP User Account	Only when LDAP authentication is used.

〔Remote Communication Gate S Pro Server > External Authentication Server (Novell) 〕: This authentication is used when logging in to RCGSP's web browser interface.

Protocol	Port	Access restriction	Note
LDAP LDAPS	389 636	EDirectory User Account	Only when Novell authentication is used.

〔Remote Communication Gate S Pro Server -> External Authentication Server (NT Authentication)〕: This authentication is used when logging in to RCGSP's web browser interface.

Protocol	Port	Access Restriction	Note
Multiple TCP/IP and NetBIOS	53 135 137 138 139 445	Domain Account	・ These ports are only used when NT Authentication is set as the authentication method. ・ The port used is determined by Windows internal specifications.

〔Remote Communication Gate S Pro Server -> External Authentication Server (Active Directory Authentication)〕: This authentication is used when logging in to RCGSP's web browser interface.

Protocol	Port	Access Restriction	Note
Multiple TCP/IP and NetBIOS	53 135 137 138 139 445	Domain Account	・ These ports are only used when AD Authentication is set as the authentication method. ・ The ports listed are the standard ports, but differences may exist due to Windows Specification changes.

〔Remote Communication Gate S Pro Server-> External Authentication Server (Notes)〕: This authentication is used when logging in to RCGSP's web browser interface.

Protocol	Port	Access Restriction	Note
Selectable from multiple TCP/IP	389	Notes Account	This port is only used when Notes is set as the authentication. The exact protocols used depends on Notes' application settings.

5-1-20 Network Traffic Estimates

〔Average Traffic volume between one device and the Remote Communication Gate S Pro Server (Reference)〕

Pattern

Device Search was performed using the following settings:

1. Search target device： Network device
2. Protocol： SNMPv3 priority
3. Search method：Network Search
   Communication Traffic:
   0.364MB/Sec（Average value for 30 minutes）

NOTE: *This example is for device Discovery.*

6. Attention

- It is recommended that the device access account, the Read Community Name, and the Read/Write Community Name be changed from their default values. If the default value is used, an unauthorized administrator will be able to easily gain access to device settings. Therefore, using RCGSP's batch configuration function to change each registered devices' community name and device access account is highly recommended.

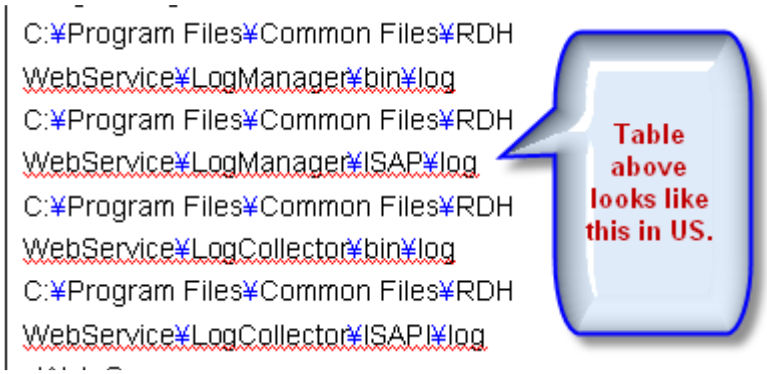
- When updating firmware, the device access account's password is encrypted using MD5. Since MD5 hashes the password, a hacker using a packet capture can only collect the hashed password. Also, users on an external network cannot initiate a firmware update operation, so external hack attempts should not present a problem.

7. Data Flow and Data Storage

7-1 Data Storage

Data	Security Spec
DeviceDatabase	Data is stored in the SQL database. A fixed Account/Password is used to access the SQL Server. The SQL SA (System Administrator) password is determined during installation. The DB is protected by a password. This data is included in the administrator-generated backup data. Backup data is stored at the location selected by the RCGSP Admin during the backup process. Backup data is information is encrypted using SHA1.
JobLog/AccessLog Database	Data is stored in the SQL database. A fixed Account/Password is used to access the SQL Server. The SA password is determined during installation. The DB is protected by a password.
Firmware Database	Firmware data is stored on the RCGSP server. Path: C:\ProgramFiles\Common Files\RDH WebService\MngCore\firmwares
Package Database	Package data is stored on the RCGSP server. Path: C:\Program Files\Common Files\RDH WebService\softmanage\data
SysLogData	Data is stored in the SQL database. A fixed Account/Password is used to access the SQL Server. The SA password is determined during installation. The DB is protected by a password.
Administrator Account Information	Administrator Account information is stored in RCGSP's internal database, and password information is encrypted using DES. Account information is accessed over SOAP using the user name and password entered at login.
- SQL Server Instance name - SQL Server DB name - SQL Server Account	The information is stored on the RCGSP server. Path: C: \Program Files\RMWSDMEX\bin\WsdmSCM.ini
-Read Community Name -Read/Write Community Name -Device Access Account -Discovery Settings	This information is stored in the SQL database. A fixed Account/Password is used to access the SQL Server. The SA password is determined during installation. The database is protected by a password. This data is included in the administrator-generated backup data. Backup Data is stored at the location selected by the RCGSP Admin during the backup process.
Ricoh_Private_MIB Information	This information is stored on the RCGSP server. It is encrypted using a common method. Path: C:\Program files\Common Files\RDH WebService\MngCore\Conf

Data	Security Spec
Logs for Debugging The log collection tool can be found in C:\Program Files\RMWSDMEX\bin\DebugLogCollector.zip	Logs are stored on the RCGSP server. This information is not encrypted. Path: < Device Management, Software Management > C:\Program Files\Common Files\RDH WebService\MngCore C:\Program Files\Common Files\RDH WebService\MngCore\logs C:\Program Files\Common Files\RDH WebService\MngCore\bin <Log Management> C:\Program Files\Common Files\RDH WebService\LogManager\bin\log C:\Program Files\Common Files\RDH WebService\LogManager\ISAP\log C:\Program Files\Common Files\RDH WebService\LogCollector\bin\log C:\Program Files\Common Files\RDH WebService\LogCollector\ISAPI\log <Web Server> C:\Program Files\Common Files\RDH Shared2\bin\log C:\Program Files\Common Files\RDH Shared2\Tomcat\logs <Application, Tools> C:\Program Files\RMWSDMEX\bin C:\Program Files\RMWSDMEX\bin\log C:\Program Files\RMWSDMEX\bin\log\ui_log <SQL Server> C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL C:\Program Files\Microsoft SQL Server\90\Setup Bootstrap\LOG



7-2 Other

Events generated by the database

Event	Cause and Action
The message "Warning capacity of SQL database exceeded!" appears.	These messages appear when the SQL database's capacity has been exceeded. If either the Job or Access log, or some combination of them exceeds 3.6 GB, the SQL database will consider itself full and the database will stop accepting more data. This is the result of a limitation in SQL. <Suggested Actions> Use the [System Log for Device Log Collection] (p.106 "System Log for Device Log Collection") to check the SQL database's current capacity and, if necessary, delete unnecessary logs in [Log Management] [Service Settings] (p.74 "Log Management Service Settings") - [Log Batch Deletion...]. Also, shorten the storage period in [Log Management Service Settings] - [Specify Log Storage Period...] in order to reduce the amount of data in the MSDE database.
The message "System suspension capacity of SQL database exceeded!" appears.	

8. JobLog / AccessLog Export Data

Job Log and Access Log information will be added to this White Paper in the next release.